The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

04/13/2011

SUBJECT:

Vulnerability in Microsoft HTML Help Could Allow Remote Code Execution

OVERVIEW:

A vulnerability has been discovered in Microsoft HTML Help which could allow remote code execution. Microsoft HTML Help allows users to view HTML help files for Windows operating systems. The vulnerability can be exploited if a user opens a specially crafted Microsoft HTML Help file. The file may be received as an email attachment, or downloaded via the web. Successful exploitation will result in an attacker gaining the same privileges as the logged on user within the context of the application. Depending on the privileges associated with the user, the attacker could then install programs; view, change, or delete data; or create new accounts with full privileges.

There is currently no patch available to remediate this vulnerability. Proof of concept code is publicly available.

SYSTEMS AFFECTED:
- Windows XP
- Windows 7
- Windows Server 2003
- Windows Vista
- Windows Server 2008

RISK:

Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:

A stack-based buffer overflow vulnerability has been discovered in Microsoft HTML Help. This vulnerability exists due to the way Microsoft HTML Help processes MicrosoftHTML Help (.chm) files. Specifically, the file responsible for decompressing Microsoft HTML Help files, ‘itss.dll’, fails to perform boundary checks before copying user-supplied data into buffers. This process occurs during the decompression of LZX chunks of files embedded in a specially crafted '.chm' help file.

This vulnerability could allow remote code execution if a user opens a specially crafted Microsoft HTML Help file. The file may be received as an email attachment, or downloaded via the web. Successful exploitation will result in an attacker gaining the same privileges as the logged on user within the context of the application. Depending on the privileges associated with the user, the attacker could then install programs; view, change, or delete data; or create new accounts with full privileges.

There is currently no patch available to remediate this vulnerability. Proof of concept code is publicly available.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches when available by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Do not visit untrusted websites or follow links provided by unknown or untrusted sources.
- Do not open email attachments from unknown or untrusted sources.
- Consider implementing file extension whitelists for allowed e-mail attachments.

REFERENCES:

Security Focus:

http://www.securityfocus.com/bid/47330
http://www.securityfocus.com/archive/1/517441